Prepared for: Technical Review
Focus: Modern TLS cipher suites
Date: March 22, 2026

Detailed Report on Recommended TLS 1.2 Cipher Suites

Coverage of ECDHE, DHE, RSA/ECDSA authentication, and AES-GCM / ChaCha20-Poly1305 transport security

This report analyzes nine modern cipher suites commonly used in TLS deployments. The suites share a common goal: providing forward secrecy, authenticated encryption, and practical interoperability across browsers, APIs, gateways, and server-side applications.

Executive Summary

What these suites have in common

- All use authenticated encryption (AES-GCM or ChaCha20-Poly1305).
- All provide forward secrecy through ephemeral key exchange.
- All are widely regarded as modern, secure choices when configured correctly.

Key recommendation

Prefer ECDHE-based suites first, with ChaCha20-Poly1305 included for devices without AES acceleration. Keep DHE suites only as compatibility fallbacks where required.

BOTTOM LINE

ECDHE + AES-GCM or ChaCha20-Poly1305 is the modern baseline.

RSA and ECDSA describe server authentication certificates; ECDHE or DHE describes the key exchange; AES-GCM / ChaCha20-Poly1305 describes the record protection layer.

Suite-by-Suite Analysis

01 ECDHE-ECDSA-AES128-GCM-SHA256

Forward secrecy with ECDSA certificates, AES-128-GCM confidentiality/ integrity, SHA-256 handshake hashing.

02 ECDHE-RSA-AES128-GCM-SHA256

Forward secrecy with RSA certificates, AES-128-GCM, and SHA-256. Common interoperability choice.

03 ECDHE-ECDSA-AES256-GCM-SHA384

ECDSA auth with stronger AES-256-GCM encryption and SHA-384; higher security margin, slightly more CPU cost.

04 ECDHE-RSA-AES256-GCM-SHA384

RSA auth with AES-256-GCM and SHA-384. Strong modern suite for broad compatibility.

05 ECDHE-ECDSA-CHACHA20-POLY1305

ECDSA auth with ChaCha20-Poly1305, excellent on mobile and systems without AES acceleration.

06 ECDHE-RSA-CHACHA20-POLY1305

RSA auth with ChaCha20-Poly1305. Performance-friendly and widely supported in modern clients.

07 **DHE-RSA-AES128-GCM-SHA256**

Finite-field DHE with RSA auth, AES-128-GCM, and SHA-256. Forward secrecy, but generally less efficient than ECDHE.

08 **DHE-RSA-AES256-GCM-SHA384**

Finite-field DHE with RSA auth and AES-256-GCM. Strong, but typically slower than elliptic-curve alternatives.

09 **DHE-RSA-CHACHA20-POLY1305**

Finite-field DHE with RSA auth and ChaCha20-Poly1305. Good fallback in some legacy stacks.

Comparison Matrix

#	Cipher Suite	Auth	Key Exchange	Bulk Cipher	Typical Strengths	Notes
1	ECDHE-ECDSA-AES128-GCM-SHA256	ECDSA	ECDHE	AES-128-GCM	Fast, compact certificates, strong default	Excellent when ECDSA certs are available
2	ECDHE-RSA-AES128-GCM-SHA256	RSA	ECDHE	AES-128-GCM	Broad compatibility	Common choice for mixed-client environments
3	ECDHE-ECDSA-AES256-GCM-SHA384	ECDSA	ECDHE	AES-256-GCM	Higher security margin	Best where clients support it and performance is acceptable
4	ECDHE-RSA-AES256-GCM-SHA384	RSA	ECDHE	AES-256-GCM	Strong security + compatibility	Often used in enterprise default policies
5	ECDHE-ECDSA-CHACHA20-POLY1305	ECDSA	ECDHE	ChaCha20-Poly1305	Great on mobile / no AES-NI	Very efficient on software-only crypto
6	ECDHE-RSA-CHACHA20-POLY1305	RSA	ECDHE	ChaCha20-Poly1305	Modern fallback with broad support	Excellent cross-platform compatibility
7	DHE-RSA-AES128-GCM-SHA256	RSA	DHE	AES-128-GCM	Forward secrecy in older stacks	Less efficient than ECDHE; keep for compatibility only
8	DHE-RSA-AES256-GCM-SHA384	RSA	DHE	AES-256-GCM	Strong legacy-compatible option	Prefer strong DH parameters if used
9	DHE-RSA-CHACHA20-POLY1305	RSA	DHE	ChaCha20-Poly1305	Software-efficient legacy fallback	Usually lower priority than ECDHE suites

Deployment Guidance

Preferred order

For most servers, an ordering such as ECDHE-ECDSA-AES128-GCM, ECDHE-RSA-AES128-GCM, ECDHE-ECDSA-CHACHA20, ECDHE-RSA-CHACHA20, then AES-256 variants is reasonable.

Certificate strategy

If your environment supports ECDSA certificates, they can reduce handshake size and often improve efficiency. RSA remains the compatibility anchor for older ecosystems.

Performance note

AES-GCM is typically fastest on hardware with AES acceleration. ChaCha20-Poly1305 is especially attractive on mobile devices and virtualized environments.

Security hygiene

Avoid static RSA key exchange, RC4, 3DES, EXPORT suites, and unauthenticated ciphers. Use strong curves, current certificate chains, and modern protocol settings.

Practical Ranking

1. **ECDHE-ECDSA-AES128-GCM-SHA256** — best balance of speed and security when ECDSA is available.
2. **ECDHE-RSA-AES128-GCM-SHA256** — best compatibility-focused default.
3. **ECDHE-ECDSA-CHACHA20-POLY1305** — ideal for software-only or mobile-heavy environments.
4. **ECDHE-RSA-CHACHA20-POLY1305** — strong modern fallback.
5. **ECDHE-ECDSA-AES256-GCM-SHA384** — use where higher crypto margin is preferred.
6. **ECDHE-RSA-AES256-GCM-SHA384** — strong enterprise-compatible option.
7. **DHE-RSA-AES128-GCM-SHA256** — compatibility fallback.
8. **DHE-RSA-AES256-GCM-SHA384** — compatibility fallback with more overhead.
9. **DHE-RSA-CHACHA20-POLY1305** — niche fallback where ECDHE is unavailable.

This report is intended for security planning and configuration review. Final cipher selection should be tested against your client population and policy requirements.